

App # 09/706,728 in Reply to Office Action Aug. 24, 2007 -2nd Supplementary Amendment June 27, 2008 Page - 2

RECEIVED
CENTRAL FAX CENTER
JUN 27 2008

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application. Claim 15 is presented on page 6 in unmarked form for Examiner's convenience.

Listing of Claims:

1 Claims 1-14 (Cancelled)

1 15. (currently amended) An encryption circuit for simultaneously processing various
2 encryption algorithms, the encryption circuit adapted to be coupled to a host computer
3 system, the encryption circuit comprising:
4 an input/output module coupled to the host computer system ~~via~~through a dedicated
5 bus,
6 the input/output module handling data exchanges between the host system and the
7 encryption circuit ~~via the input/output module and the dedicated bus and,~~
8 the input/output module comprising a microcontroller and a microcontroller
9 control memory, the microcontroller control memory providing storage for
10 program control of the microcontroller;
11 an encryption module ~~coupled to the input/output module,~~
12 ~~said encryption module controlling~~ performing data encryption and decryption
13 operations, as well as storage of all sensitive information of the encryption
14 circuit; and
15 isolation means ~~operatively comprising~~ a dual port memory connected between the
16 input/output module and the encryption module, the isolation means
17 ~~configured to make~~ ensuring that the sensitive information stored in the
18 encryption module ~~is~~ inaccessible to the host computer system,
19 ~~and for ensuring the operations performed by the input/output module and~~
20 ~~encryption module can be carried out in parallel~~
21 ~~the dual port memory enabling parallelism between 1) the data exchanges~~
22 ~~performed by the input/output module and 2) the data encryption and~~
23 ~~decryption operations performed by the encryption module.~~

App # 09/706,728 In Reply to Office Action Aug. 24, 2007 -2nd Supplementary Amendment June 27, 2008 Page - 3

1 Claims 16-19 (Canceled)

1 20. (currently amended) An encryption circuit as set forth in claim [17] 15, wherein the
2 encryption module comprises:

3 a first encryption sub-module, dedicated to the processing of symmetric encryption
4 algorithms, and being coupled to the first bus of the dual port memory;

5 a second encryption sub-module, dedicated to the processing of asymmetric
6 encryption algorithms and being coupled to the first bus of the dual-port memory
7 and including a separate internal second bus isolated from the first bus of the dual-
8 port memory; and

9 a CMOS memory, coupled with the dual-port memory via the first bus of the dual-
10 port memory, the CMOS memory containing the encryption keys accessible during
11 execution of encryption algorithms by the first and second encryption sub-modules
12 and the CMOS memory connected to be reset upon detection of an alarm condition
13 protecting the encryption keys from unauthorized access and use.

1 21. (currently amended) An encryption circuit according to claim [18] 20, wherein
2 the first encryption sub-module comprises an encryption component coupled to the dual-
3 port memory via the first bus of the memory, the encryption component comprising
4 various encryption automata, respectively dedicated to the processing of symmetric
5 encryption algorithms, and the second encryption sub-module comprises at least two
6 encryption processors, respectively dedicated to the processing of asymmetric encryption
7 algorithms, the encryption processors being coupled to the first bus of the dual-port
8 memory via the internal second bus of the second sub-module and a bus isolator that
9 isolates the second bus from the first bus of the dual-port memory.

App # 09/706,728 in Reply to Office Action Aug. 24, 2007 -2nd Supplementary Amendment June 27, 2008 Page - 4

- 1 22. (Previously Presented) An encryption circuit according to claim 21, wherein the
2 encryption processors of the encryption module are of the CIP configuration.
- 1 23. (Previously Presented) An encryption circuit according to claim 21, wherein one of
2 the two encryption processors is of the CIP type, and in that the other of the two
3 encryption processors is of the ACE configuration.
- 1 24. (Previously Presented) An encryption circuit according to claim 21, wherein one of
2 the two encryption processors is of the ACE configuration comprising a field
3 programmable gate array (FPGA).
- 1 25. (Previously Presented) An encryption circuit according to claim 24, wherein the
2 encryption component is of the SCE configuration.
- 1 26. (Previously Presented) An encryption circuit according to claim 25, wherein the
2 encryption component comprises a field programmable array (FPGA).
- 1 27. (Previously Presented) An encryption circuit according to claim 26, wherein the
2 second encryption sub-module comprises a flash memory PROM and an SRAM memory
3 coupled to the second internal bus of the sub-module.
- 1 28. (Previously Presented) An encryption circuit according to claim 21, further
2 comprising a CMOS memory containing security keys and security mechanisms that
3 trigger a reset mechanism of the CMOS memory in case of an alarm protecting the
4 encryption keys from unauthorized access and use.

App # 09/706,728 in Reply to Office Action Aug. 24, 2007 -2nd Supplementary Amendment June 27, 2008 Page - 5

- 1 29. (Previously Presented) An encryption circuit according to claim 15, wherein the
- 2 microcontroller comprises:
 - 3 an input/output processor and a PCI interface integrating DMA channels responsible
 - 4 for executing the data transfers between the host computer system and the circuit; and
 - 5 the memory comprises a flash memory containing the code of the input/output
 - 6 processor and a static random access memory that receives a copy of the contents of
 - 7 the flash memory upon startup of the input/output processor.
- 1 30. (Previously Presented) An encryption circuit according to claim 15, comprising a
- 2 serial link connected to input basic keys through a secure path independent of the
- 3 dedicated PCI bus, said link controlled by the encryption module.
- 1 31. (Previously Presented) An encryption circuit according to claim 30, wherein the
- 2 serial link (SL) allows downloading of proprietary algorithms into the first encryption
- 3 sub-module.
- 1 32. (Original) An encryption circuit as set forth in claim 15, further including a card
- 2 supporting the circuit.
- 1 33. (Original) An encryption circuit as set forth in claim 18, further including a card
- 2 supporting the circuit.
- 1 34. (Original) An encryption circuit as set forth in claim 21, further including a card
- 2 supporting the circuit.

App # 09706,728 in Reply to Office Action Aug. 24, 2007 -2nd Supplementary Amendment June 27, 2008 Page - 6

1 35. (New) An encryption circuit for simultaneously processing various encryption
2 algorithms, the encryption circuit adapted to be coupled to a host computer system, the
3 encryption circuit comprising:
4 an input/output module coupled to the host computer system through a dedicated bus
5 which provides direct access by the encryption circuit to the host system,
6 the input/output module handling data exchanges between the host system bus
7 and the encryption circuit;
8 the input/output module comprising a microcontroller and a microcontroller
9 control memory, the microcontroller control memory providing storage
10 for program control of the microcontroller;
11 an encryption module performing data encryption and decryption operations, as
12 well as storage of all sensitive information of the encryption circuit, the
13 encryption module comprising:
14 a first encryption sub-module, dedicated to the processing of symmetric
15 encryption algorithms;
16 a second encryption sub-module, dedicated to the processing of
17 asymmetric encryption algorithms; and
18 a CMOS memory containing the encryption keys accessible during
19 execution of encryption algorithms by the first and second encryption sub-
20 modules and the CMOS memory connected to be reset upon detection of an
21 alarm condition protecting the encryption keys from unauthorized access and
22 use; and
23 isolation means comprising a dual port memory connected between the input/output
24 module and the encryption module, the dual port memory being coupled to a
25 first bus which couples to the first encryption sub-module, said second
26 encryption sub-module and a second bus which couples to the input/output
27 module, the isolation means ensuring that the sensitive information stored in
28 the encryption module is inaccessible to the host computer system and is
29 protected from unauthorized access and use, and
30 the dual port memory enabling a first level of parallelism between 1) the data
31 exchanges performed by the input/output module and 2) the data
32 encryption and decryption operations performed by the encryption
33 module; and
34 a second level of parallelism by providing access to data of the dual port memory
35 during parallel operation of both first and second encryption sub-modules.

App # 09/706,728 in Reply to Office Action Aug. 24, 2007 -2nd Supplementary Amendment June 27, 2008 Page - 7

Claim 15 – presented as amended without markup (for Examiner's convenience):

- 1 15. (currently amended) An encryption circuit for simultaneously processing various
- 2 encryption algorithms, the encryption circuit adapted to be coupled to a host computer
- 3 system, the encryption circuit comprising:
 - 4 an input/output module coupled to the host computer system through a dedicated
 - 5 bus,
 - 6 the input/output module handling data exchanges between the host system and the
 - 7 encryption circuit,
 - 8 the input/output module comprising a microcontroller and a microcontroller
 - 9 control memory, the microcontroller control memory providing storage for
 - 10 program control of the microcontroller;
 - 11 an encryption module performing data encryption and decryption operations, as well
 - 12 as storage of all sensitive information of the encryption circuit; and
 - 13 isolation means comprising a dual port memory connected between the input/output
 - 14 module and the encryption module, the isolation means ensuring that the
 - 15 sensitive information stored in the encryption module is inaccessible to the
 - 16 host computer system,
 - 17 the dual port memory enabling parallelism between 1) the data exchanges
 - 18 performed by the input/output module and 2) the data encryption and
 - 19 decryption operations performed by the encryption module.